(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 April 2004 (08.04.2004)

PCT

(10) International Publication Number
WO 2004/030294 A1

(51) International Patent Classification⁷: H04L 12/56

(21) International Application Number: PCT/KR2003/002001

(22) International Filing Date: 30 September 2003 (30.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02 1 44083.2 30 September 2002 (30.09.2002) CN

(71) Applicants (*for all designated States except US*): **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR). **BEIJING SAMSUNG TELECOM R & D CENTER** [CN/CN]; 4F Science and Technology Tower, No.11 Zhongguancun Nan Lu, Haidian District, Beijing 100081 (CN).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **ZHU, Yanmin** [CN/CN]; 4F Science and Technology Tower, No.11 Zhongguancun Nan Lu, Haidian District, Beijing 100081 (CN).

(74) Agent: **LEE, Keon-Joo**; Mihwa Bldg., 110-2, Myongryun-dong 4-ga, Chongro-gu, Seoul 110-524 (KR).

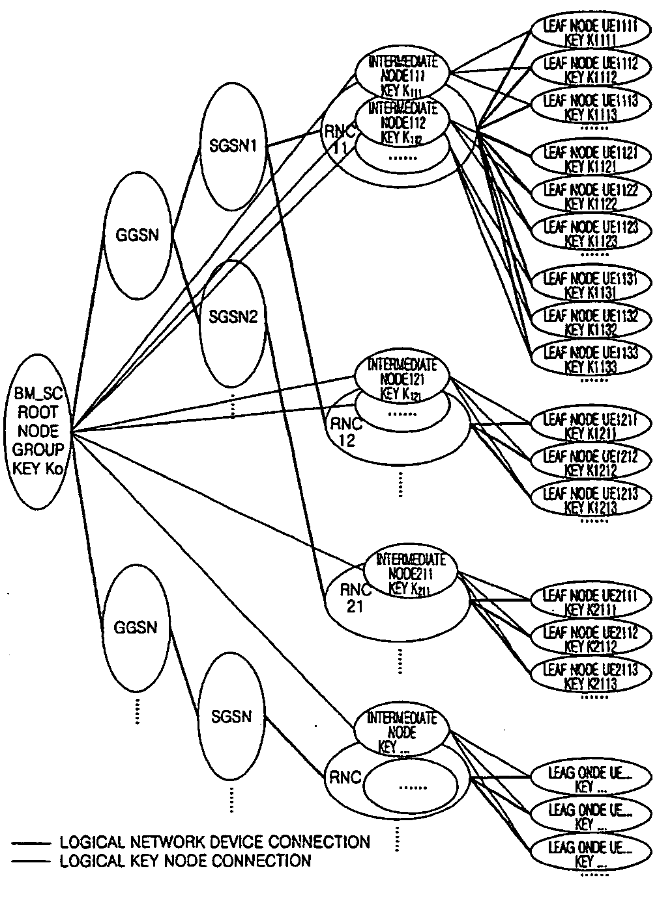
(81) Designated States (*national*): JP, KR, US.

(84) Designated States (*regional*): European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CIPHERING KEY MANAGEMENT AND DISTRIBUTION IN MBMS


LEAF NODE UE1111 KEY K1111
INTERMEDIATE NODE111 KEY K111
LEAF NODE UE1112 KEY K1112
INTERMEDIATE NODE112 KEY K112
LEAF NODE UE1113 KEY K1113
SGSN1
RNC 11
LEAF NODE UE1121 KEY K1121
LEAF NODE UE1122 KEY K1122
GGSN
LEAF NODE UE1123 KEY K1123
LEAF NODE UE1131 KEY K1131
SGSN2
LEAF NODE UE1132 KEY K1132
LEAF NODE UE1133 KEY K1133
INTERMEDIATE NODE121 KEY K121
BM_SC ROOT NODE GROUP KEY Ko
RNC 12
LEAF NODE UE1211 KEY K1211
LEAF NODE UE1212 KEY K1212
LEAF NODE UE1213 KEY K1213
INTERMEDIATE NODE211 KEY K211
RNC 21
LEAF NODE UE2111 KEY K2111
GGSN
LEAF NODE UE2112 KEY K2112
LEAF NODE UE2113 KEY K2113
SGSN
INTERMEDIATE NODE KEY ...
RNC
LEAG ONDE UE... KEY ...
LEAG ONDE UE... KEY ...
LEAG ONDE UE... KEY ...
LOGICAL NETWORK DEVICE CONNECTION
LOGICAL KEY NODE CONNECTION

(57) Abstract: A method for key management and assignment in MBMS service, the method includes following steps: the group key locates in the root node on the highest layer, which only has child nodes and doesn't have parent nodes; private keys corresponding to users locate in leaf nodes; the described intermediate node that owns both one parent node and one or more child nodes holds it own key. This invention deploys the method of combining point-to-point mode and point-to-multipoint mode during the process of key update; compared with the key update method only deploying point-to-point mode, this method can reduce the times necessary for information transmission, reduce the system load as well as the time needed for one key update process. Compared with the key update method only deploying point-to-multipoint mode, this solves the security problem of key exposure.